An Expandable Montgomery Modular Multiplication Processor

Gutub, A.A.A. Amin, A.A.M.; Dept. of Comput. Eng., King Fahd Univ. of Pet. & Miner., Dhahran, Saudi Arabia;

Microelectronics, 1999. ICM '99. The Eleventh International conference;Publication Date: 22-24 Nov. 1999;ISBN: 0-7803-6643-3

King Fahd University of Petroleum & Minerals

http://www.kfupm.edu.sa

Summary

Several public-key cryptographic systems (Schneier, 1996) make heavy use of modular multiplication. A design for expandable modular multiplication hardware is proposed. This design allows for cascading the hardware if larger moduli are required. The proposed design uses a Montgomery modular multiplication algorithm (Koc et al, IEEE Micro, pp. 26-33, June 1996).